5 FAM 770
FEDERAL WEBSITES

(TL:IM-48; 01-09-2004)
(Office of Origin: A/RPS/DIR)

5 FAM 771 DEFINITION

(TL:IM-33; 02-27-2002)

Department websites created for both the general public and internal Department viewing are considered Federal websites. This includes websites on classified and unclassified networks.

5 FAM 772 PRIVACY PRINCIPLES FOR FEDERAL WEBSITES

5 FAM 772.1 Overall

(TL:IM-33; 02-27-2002)

a. Web site managers, web page designers, and program offices must ensure that the privacy of personal information is protected.

b. Federal web sites must include a privacy policy statement, even if the site does not collect any information that results in creating a Privacy Act record.

c. The Privacy Act of 1974 requires a privacy notice when collecting personal data from individuals that is stored in a system of records keyed to personal identifier or other identifying symbol assigned to an individual. The Privacy Act also limits the disclosure of personal information.

d. Information placed on a web site is subject to the same Privacy Act restrictions as when releasing non-electronic information. A privacy notice is required for the web site as a whole to cover web site issues such as logs, emails to the webmaster and other specific issues. Direct specific privacy questions to the Department's Privacy Act Office, A/RPS/IPS.

e. The extent of the use of personally identifying information must be fully

disclosed and protections must be put in place to ensure information is used only within the expectations and understanding of the public. Information collected for one purpose may not be used for another purpose without notice to or consent of the subject of record. When gathering information from the public, security in the form of encryption and digital certificates must be integrated into the applications to the greatest extent possible.

f. Information obtained to conduct system administration functions must be protected. System administrators must maintain the confidentiality of the contents of electronic communications and prevent disclosure of electronic communications to avoid being in violation of the Electronic Communications Privacy Act.

g. All Federal web sites and contractors, when operating on behalf of agencies, shall comply with the standards set forth in the Children's Online Privacy Protection Act of 1998 with respect to the collection of personal information online at web sites directed to children.

5 FAM 772.2 Links to Internet Web Sites

(TL:IM-33; 02-27-2002)

a. Internet to Internet—When linking from Department Internet web pages to locations outside of Federal government domains, disclaimers must be added to advise the public that the Department is not responsible for and does not endorse the non-government organization. Suggested text, or its equivalent: "This site is produced and maintained by the [optional-list section, office or bureau] U.S. Department of State. Links to other sites are provided as a convenience and should not be construed as an endorsement of the views or products contained therein."

b. Intranet to Internet—When linking from a Department intranet, such as OpenNet Plus, to an Internet location, a warning notice must be added to alert the user that the new location is outside the Department's private network.

5 FAM 773 INTERNET WEB SITE HOSTING

(TL:IM-33; 02-27-2002)

a. For domestic audiences, the Bureau of Public Affairs (PA) publishes public foreign policy material and information about the State Department on the Internet for all bureaus and provides some publishing services for

selected operational entities.

b. For audiences abroad, posts should either contract with a local Internet service provider, host the site internally, or work with the Coordinator, International Information Programs, Office of Electronic Media (IIP/T/EM), for other alternatives or to host the site in Washington.

c. All offices maintaining a web site, whether managed by that office, another Department office, or a contractor; will have an e-mail address which visitors to the office web site can use to make comments and/or ask questions. The e-mail address should be generic to the office or staff function and not that of an individual employee or contractor.

5 FAM 774 CLASSNET WEB SITE CLASSIFICATION MARKING

(TL:IM-48; 01-09-2004)

a. Classified, restricted distribution, and SBU material will not be displayed on the Internet.

b. Classified and restricted distribution material will not be displayed on unclassified intranet web sites.

c. For classified web sites, the requirements of E.O. 12958 concerning classified information "apply regardless of physical format and to all document types." Webmasters are responsible for ensuring that the following markings appear clearly on all classified web sites.

(1) Overall classification of the page, centered at the top and bottom of the page, should be indicated by a continuous vertical marking on the left side of the page. This marking will be tiled as the page scrolls and, therefore, be visible through the whole page.

(2) Overall classification of the page should be indicated, centered at the top and bottom of the page. This marking will properly mark printed copies of the web page.

(3) Individual elements of the web page (e.g., text, images, tables, lists, etc.) should be portion marked with the highest classification contained within the element as prescribed in 12 FAM 529 for normal printed material.

(4) An appropriate declassification instruction should be displayed at the bottom of the web page.

d. The <body> tag should contain the URL of the appropriate background for the classified web page.

   Example: <body background="name_of_classified_background.gif">

e. An unclassified sample secret web page modeling these requirements can be viewed on IRM's website. Background images can be downloaded following instructions on the sample web page.

5 FAM 775 INCIDENT HANDLING

(TL:IM-48; 01-09-2004)

a. Web site managers, whether they perform site monitoring activities themselves to identify security incidents or rely on the Internet service provider (ISP) for these services, must be prepared to report and respond to incidents if they occur. All incidents should be reported to the ISSO and RSO and to the following teams. Site managers should:

   (1) Immediately report any suspected virus activity on any system to the Virus Incident Response Team (VIRT). They should also submit the virus report, available on OpenNet, to the Systems Integrity Division (IRM/OPS/ITI/SI) each time a virus is discovered. The complete anti-virus program description is also available on the VIRT website.

   (2) Immediately report to the Computer Incident Response Team (CIRT) unsolicited or junk commercial e-mail ("spam"), anonymous e-mail, denial-of-service attacks, or suspicious attachments that may be sent to Department e-mail addresses, including any addresses associated with the web site. The CIRT may be reached by e-mail at CIRT@state.gov. Should e-mail be unavailable, an alternate point of contact is the IRM Infocenter.

   (3) Report attempts to thwart or bypass security, whether successful or unsuccessful, to the CIRT. These include web site related incidents such as: attempts to access and/or change web site content, passwords, etc.; non-web site related attacks such as excessive unauthorized logon and access attempts to the server; access attempts after regular local business hours; unauthorized access or permissions to file directories, share data and folders, or to system applications and operating systems; unauthorized logon screens or procedures; and passwords displayed in plain text.

b. Refer to 12 FAM 600, Information Security Technology, for Automated

Information Systems security requirements. For additional information contact DS/CIS/IST/ACD.

5 FAM 776 WEB SITE DEVELOPMENT

5 FAM 776.1 Software Applications

(TL:IM-33; 02-27-2002)

a. A list of recommended software applications for web site development is promulgated by the Internet Steering Committee. Offices are authorized to procure licenses to install and use any of these applications that they determine are required for web site development. Installation should be coordinated with the appropriate systems manager when administrative privilege may be required.

b. Submit requests for additions to the recommended software list by e-mail to the Internet Steering Committee at isc@state.gov.

5 FAM 776.2 Responsibilities for Internet Web Site Operators

(TL:IM-48; 01-09-2004)

a. Any office or mission that creates or "publishes" a public web site is responsible for its content, organization, and adherence to the Department's standards and practices, and federal regulations.

b. The designated editor or content manager should:

(1) Obtain all substantive clearances of content per existing Department clearance procedures for release of information to the public. Those clearances may include other mission elements, regional or functional bureaus, Diplomatic Security, Public Affairs Office of Electronic Information (PA/EI), or International Information Programs Office (IIP).

(2) Ensure that information published on their web sites is current, relevant, and accurate.

(3) Maintain Department design and content standards, including a link to the main State Internet site. Missions abroad also should provide links to appropriate sections of the IIP website.

(4) Coordinate information exclusively or primarily for domestic U.S. audiences with PA/EI.

(5) Sites abroad should inform regional bureaus and IIP of major changes in content and design.

(6) Ensure compliance with Department privacy policies for websites (i.e. privacy statements are posted and kept current, persistent cookies are not used without proper authorization and notice).

5 FAM 776.3 Content

(TL: IM-33; 02-27-2002)

a. Domestically, web pages must follow existing approval procedures regarding Department of State documents, reports, memorandums, etc. for public release. See Forms DS-1837, Request for Approval of New or Recurring Information Dissemination. The Public Affairs Office of Electronic Information (PA/EI) approves electronic information dissemination to the public.

b. Public affairs officers shall coordinate mission web publishing to foreign audiences with mission elements and the respective geographic bureau in Washington. All materials published to the mission web site should be cleared at the mission in the same manner as they would be for paper distribution unless a separate clearance process is put in place at the mission for web publishing. Missions are encouraged to consult with the International Information Programs Electronic Media Team (IIP/T/EM) regarding content and design.

c. The Department must observe legal distinctions between domestic and international dissemination of electronic programs as required by the Smith-Mundt Act.

(1) Under the Smith-Mundt Act, the Department is prohibited from domestically disseminating materials that have been prepared about the United States, its people, and its policies for dissemination abroad. This ban applies to public diplomacy programs, including the program materials created prior to the consolidation of USIA and the Department of State. Accordingly, this ban continues to apply to posting of program materials on the Internet. Program materials must be posted on the Department's international site only.

(2) The Department must not distribute, advertise, or otherwise actively make available to persons located within the United States,

web pages that contain Smith-Mundt program materials. Embassy and mission web sites abroad which serve both domestic and foreign audiences can accomplish this goal by ensuring that policy information for foreign audiences is clearly identified and separate from information and services directed primarily toward U.S. citizens.

d. The following categories of information are prohibited from being posting on publicly accessible State Department web sites:

(1) Floor plans or blue prints of U.S. Government facilities, electrical, water, or telephone diagrams detailing routes and locations of existing wires or pipes or shafts.

(2) The existence, location, types or specifications of any physical security device and/or missing, broken or failure of any security devices.

(3) Classified and Sensitive But Unclassified (SBU) material.

(4) Other restricted distribution material (i.e., NOFORN).

(5) Privacy Act information (e.g., personal information relating to U.S. citizens, such as social security account numbers, dates of birth).

(6) Home addresses and home or cellular telephone numbers of individuals.

(7) Duty rosters or detailed organizational charts below the level of a domestic office or, at post, below the level of a key officer as stated in the Key Officers of Foreign Service Posts publication. Employee information below the level of a domestic office or below the key officer at post may be published when required by law or regulation or when public release has been specifically authorized.

(8) Personal medical records.

(9) Financial disclosure reports of U.S. Government employees.

(10) Any information about personal legal problems.

(11) Internal Department of State personnel rules and practices when they refer to specific individuals.

(12) Any information dealing with investigative actions concerning a specific person.

(13) Action on reports of selection boards when it refers to specific individuals.

(14) Labor union representation rights and duties when they refer to specific individuals.

(15) Civil and/or Foreign Service examination and/or confidential records.

(16) Drug abuse prevention and/or rehabilitation records.

(17) Software or technical information that could put Department resources at risk, such as network diagrams or port scanners.

e. The following categories of information are prohibited from being posted on publicly accessible State Department web sites, except in cases where public release has been specifically authorized:

(1) Financial records of the Department or the U.S Government

(2) Distribution lists.

(3) Shipping and receiving documents.

(4) Photographs of U.S. Government individuals, except for DCM rank and above, or as approved for public diplomacy or public affairs purposes.

(5) Biographies of U.S. Government employees except for DCM rank or equivalent and above or as required by law or approved for public diplomacy or public affairs purposes.

(6) Pictures of U.S. Government facilities, including, and of particular concern, the display of security countermeasures. A mission, however, may carry an official photograph of the embassy or chancery building.

(7) Job titles and/or descriptions of U.S. Government personnel, except as stated in the Key Officers of Foreign Service Posts publication or when required by law or regulation.

(8) Information identifying employees of other agencies, except when authorized.

(9) Travel itineraries of individuals or groups, including ambassadorial schedules, prior to the event unless previously released to the media or otherwise authorized as part of a public diplomacy or

public affairs function.

f. Posting any of the following is prohibited:

(1) Offensive or harassing material;

(2) Abusive or objectionable language;

(3) Misrepresentations of the Department; or

(4) Personal and/or commercial advertising.

g. Web site editors and content managers are responsible to ensure that their web site does not endorse or indicate preferential treatment for any product. No payment or reimbursement of any kind shall be accepted in exchange for links on an official State Department web site.

h. The English language will be used throughout all U.S. domestic web pages on the Internet and on all intranet pages regardless of audience. Foreign language translations of documents may be included with the English original, if required, to meet the purpose of the web site.

i. Posts have a foreign and domestic audience since the U.S. public is a key user of their sites. Post web sites should, therefore, have text available in English in addition to any other language for all official policy statements, and for the types of information defined in section 1461 (a) of the Smith-Mundt Act, as follows: "information about the United States, its people, and its policies disseminated through press, publications, radio, motion pictures, and other information media, and through information centers to be available, on request, in the English language at the Department of State, at all reasonable times following its release as information abroad, for examination only by representatives of United States press associations, newspapers, magazines, radio systems, and stations, and by research students and scholars…"

j. Material pertinent to internal Department operations or procedures should be posted on the intranet, not to public Internet sites. Due to FOIA requirements, some administrative materials, manuals, and instructions must be posted publicly. The FAM, FAH, and other policies that may affect the public are part of this requirement. Contact A/RPS/IPS for guidance prior to posting internal Department documents.

k. Web sites should be tested using several popular browsers to ensure faultless accessibility to everyone. State Department web sites shall not require or encourage users to choose any specific browser.

l. Graphics or logos depicting companies and/or products may be displayed

on the home page when they indicate compliance with a standard such as "Bobby Approved" for Section 508 of the Rehabilitation Act and "VeriSign" for encryption, or when they are commonly accepted utility applications such as Adobe Acrobat which may be necessary for the user to access the web site content.

Graphics or logos depicting non-commercial organizations may be used in conjunction with appropriate text to identify links to resources. This practice should be confined to a separate page labeled "References" or "Links" or some similar title. Generally all other uses of companies/product logos should not appear on the State Department's Internet or Intranet web sites.

m. The use of commercial endorsements, sponsorships, or similar items should be discussed with PA/EI or IIP. If necessary, those offices will clear such requests with the Office of the Legal Adviser.

n. Exercise caution when using informal "surveys" or forms. If you are asking the public for information, be aware of the requirements of the Paperwork Reduction Act of 1995 (PRA). The PRA does not differentiate between information collection domestically or abroad, or between U.S. citizens and foreigners. The PRA requires that all information collection requests (a request for information from 10 or more persons), with minor exceptions, must be cleared by OMB and display an OMB control number prior to issuance. A request to send feedback on the site to the webmaster is exempt. Contact the Directives Management staff in A/RPS/DIR for further assistance and authorization concerning the PRA, information collections, and OMB clearance.

o. All sites should link to the disclaimer page at http://www.state.gov/documents/ContactUs.cfm. Additional disclaimers may be added, as appropriate. If your office cannot link to this U.S. site, your office should post similar disclaimers derived from those contained on this site. The Office of the Legal Adviser should be included in the review of notices and disclaimers. Service agreements with external Internet service providers (ISP) must state that the ISP will not sell lists of users who access the Department site to any other person or entity, which would be a violation of the Privacy Act.

p. References to web contractors or hosting services should not appear on the homepage. If applicable, the web site should include a separate page labeled "Credits" or "About This Site" which provides information about web contractors, and other commercial or technical support for the web site.

q. Copyrighted information should be used only in accordance with current

copyright laws that in most cases require permission from the copyright owner. Refer to 5 FAM 480, Use of Copyrighted Material, for specific policy regarding copyrighted information.

5 FAM 776.4 Design Standards for People With Disabilities

(TL:IM-48; 01-09-2004)

a. All State Department web sites must be accessible to the disabled. Web site editors and content managers are responsible for ensuring that their web sites are tested with one or more of the recommended tools and corrections made to achieve an acceptable access level. The IRM Business Center (IRM/M/CST/BC) maintains the IMPACT intranet site, including resources to evaluate web site compliance with Section 508 of the Rehabilitation Act as amended in 1998. Other resources include the Justice Department Section 508 website; the Architectural and Transportation Barriers Compliance Board; and the Federal IT Accessibility Initiative.

b. Contact the Office of the Legal Adviser (L/EMP) and the IRM IMPACT Office (IRM/M/CST/BC) for advice and assistance on disability issues.

5 FAM 777 THROUGH 779 UNASSIGNED